Netintelligence

OPINION SHEET

Through the Barricades

The demise of traditional perimeter defences.

There is a classic moment during the battle for Helm's Deep in the epic film, Lord of the Rings, the Two Towers, when King Theoden stands atop the supposedly impregnable city. Rain sodden, he surveys the massed ranks of Suraman's armies and defiantly shouts 'Is this all you've got?' A few fateful minutes, and a well placed explosive, later his confidence is shattered and replaced with fear as he realises that his fortress has been penetrated.

Whilst this may have been a marvellous piece of celluloid drama, this scene could have been replicated in the IT departments of many enterprises throughout 2004. Replace Helm's Deep with firewalls and the Orcs with trojans and viruses and you'll soon appreciate the similarities.

In terms of security and protecting our organisations, we really are still in the dark ages, and these are the plague years. Many companies hit by the SQL Slammer, NetSky and Blaster worms - and any of last year's main viruses- learned the hard way about what worked when it came to their security defences. In the main, perimeter defences such as network firewalls, gateway signature antivirus devices, and patches just about coped, but the internal networks suffered badly.

Certainly, traditional tactics are not working. Several operating systems vendors estimate that it can take approximately 20 - 30 days to deploy, implement and test a patch across an organisation's network. This is more than enough time for a destructive virus or worm to deliver its payload. In fact many of the breaches caused last year were due to remote workers and authorised visiting contractors connecting to networks without the prescribed signature updates/patches being applied and subsequently infecting desktops and servers that were still to be secured.

Firewalls, intrusion-detection systems and antivirus software all play a role in security, but as network managers have witnessed, networks are being attacked at all levels.

The answer to the problem is becoming clearer. To provide a greater level of security we have to consider both the external threats and the internal threats in tandem. The entire network must now be considered as part of the security architecture and this concept must address network and data protection differently to the historical point-product approach. Instead, we must now focus on making security a component which can be interwoven into the basic fabric of any corporate communications system, rather than an add-on to the network. By integrating control functions with security protections, a network can more effectively respond to security threats by recognising problems, quickly quarantining noncompliant systems and more rapidly containing infections.
The stark lessons from last year highlight that there is no real value in designing security policies and investing in protective technologies - if you can't ensure that they're enforced at all times. Unless you can mandate and enforce compliance across the whole extended network - both behind and beyond the traditional perimeter boundaries - you will always be fighting a losing battle.

One key challenge for the enterprise in achieving a total security system is to realise that the end point must now be considered a core network component. A total security requires endpoints and the network to communicate better so that the overall network can do a better job of protecting these valuable devices and their data.

This generally involves installing a client on every end point device which will then analyse the roles and interdependencies, and the interaction made between the device and the user, thereby providing an understanding of all the behaviours that are occurring throughout the network. Typically this new breed of end point solution encompasses configuration management, virus scanning, and host intrusion detection/ protection with distributed firewall capabilities. In essence a 'micro version' of the traditional perimeter defences, that can be applied locally. Each end point client has three distinct areas of functionality: Monitoring/Discovery, Reporting & Control. By physically residing on the end point, the client is ideally placed to view, in real time, the activities that are considered both 'appropriate' and 'inappropriate'. Where it detects behaviours which it considers 'harmful' or 'against the norm' - such as zero day threat - it can take the designated course of action immediately. This action might be: to kill all processes, isolate the machine or it may be a simple case of alerting the Sys.Admin. But whichever course the client has followed, the overall objective remains the same - keep the overall network protected and ensure that policy has not been breached. This combination of monitoring and defence technologies, hosted at the end point, is, by default, forcing all access devises to behave compliantly - wilful bypassing of policy and best practise can not occur.

For End Point security to become effective, the organisation must really take its policy setting seriously. The policy must effectively determine that only properly configured and secured endpoints may access the network, it must leverage the existing security infrastructures and investments, and it must ensure that the policy suits the individual needs of the LOBs (Lines of Business) within the organisation. Getting the policy right first time is not critically important as the policy should become an integral part of the organisation's fabric, and as such should be constantly reviewed, amended and issued.

Once you have created the policy, you will need to consider the End Point solution that best suits your needs. You will need to remember that by its very nature, End Point security requires the mass deployment of clients to each device, and that there are logistical implications to be considered. A solution which includes the purchase of specialist hardware or the manual configuration of existing systems will probably provide a significant enough barrier to entry to not get past first base. The client should ideally be physically installed on the end point, but actually operates 'invisibly' to the user. You do not want the user to be confronted with a series of 'choices' at any stage during operation e.g. do I take this course of action? Is it OK for me to do this? What will be the effect if I do this? The client should be making these decisions for the user based upon the criteria that it has been set to follow. Not only will you want the functionality to remain 'invisible' but you will also need the client to be as light on processing as possible - increased calls into the helpdesk about slow running machines will be counter productive. Furthermore, you need a solution that can't be disabled or bypassed, by end users, even if they have local administrative privileges on their PCs.
You should consider how the End Point solution integrates within your existing infrastructure, and how the two can best combine to deliver your policy. For example do you need proxy web blocking and filtering if you can now do this at the micro level on an individual by individual basis? If careful consideration is given to this area, there should be a case for substantial cost savings to be made across the whole infrastructure. It is also important to select a solution that is open standard to avoid vendor tie in and can be easily integrated with future network enhancements.

Finally, being End Point based will provide an incredibly detailed picture of the state of the network as a whole. But this information only has any relevance or use if it is actually used properly. Regular interrogation of the reporting function will provide historical, consolidated and trended views. These mechanisms will enhance the ability to analyse traffic and make dynamic, automated decisions about access, infection containment and remediation. Ultimately, the network will have the distributed intelligence to make decisions about the trust level of users and the information that they share. This data can actively be used to shape and mould the policy moving forward - taking security from away from its usual state of perpetual reaction to one of pre planning and control.

Implementing an end point solution will require some effort, convincing the traditionalists and loading clients onto every device for example, but the results will be worth it.

King Theoden was lucky, he had Gandalf and the riders of Rohan to bail him out of his predicament, you may not be so blessed!

For further details:
Netintelligence. www.netintelligence.com or email:info@netintelligence.com.
Tel: 44 (0) 870 050 0121